

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Déni de service dans Realsecure Server Sensor d'ISS

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-027>

Gestion du document

Référence	CERTA-2002-AVI-027
Titre	Déni de service dans Realsecure Server Sensor d'ISS
Date de la première version	08 février 2002
Date de la dernière version	–
Source(s)	Avis de sécurité #109 d'Internet Security Scanner
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni de service.

2 Systèmes affectés

RealSecure Server Sensor versions 6.0.1 et 6.5 sur plate-forme Windows.

3 Résumé

RealSecure Server Sensor est un détecteur d'intrusions analysant différentes sources d'informations (trafic réseau sur les interfaces, enregistrements des journaux systèmes...) sur un serveur.

Une vulnérabilité dans le traitement des paquets ICMP permet à un utilisateur mal intentionné de réaliser un déni de service par arrêt du serveur.

4 Description

En générant un nombre important de paquets ICMP de type Echo Request (`ping`) à destination d'une machine utilisant RealSecure Server Sensor, un utilisateur mal intentionné peut forcer l'arrêt brutal du serveur.

D'autres produits de l'éditeur Internet Security Systems sont également concernés par cette vulnérabilité : BlackICE Defender et BlackIce Agent Desktop (se référer à l'avis de sécurité de l'éditeur).

5 Contournement provisoire

Mettre en place un filtrage des paquets ICMP au niveau des pare-feux si la politique de sécurité le permet afin d'empêcher les attaques provenant de l'extérieur.

6 Solution

Se référer à l'avis de sécurité #109 de l'éditeur (cf. section Documentation).

7 Documentation

Avis de sécurité "Remote denial of service vulnerability in BlackICE products" d'Internet Security Systems : http://www.iss.net/security_center/alerts/advise109.php

Gestion détaillée du document

08 février 2002 version initiale.